Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2016 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-10-2016

User Archetypes for Effective Information Privacy Communication

Tobias Dehling
University of Kassel, tdehling@uni-kassel.de

Manuel Schmidt-Kraepelin
University of Cologne, schmidt-kraepelin@wiso.uni-koeln.de

Muhammed Demircan
University of Cologne, it.demircan@googlemail.com

Jakub Szefer
Yale University, jakub.szefer@yale.edu

Ali Sunyaev
University Kassel, sunyaev@uni-kassel.de

User Archetypes for Effective Information Privacy Communication

Completed Research

Tobias Dehling
Information Systems and Systems Engineering, Research Center for IS Design (ITeG),
University of Kassel, Germany {tdehling@uni-kassel.de}

Manuel Schmidt-Kraepelin
Department of Information Systems, University of Cologne, Germany
{schmidt-kraepelin@wiso.uni-koeln.de}

Muhammed Demircan
Department of Information Systems, University of Cologne, Germany
{it.demircan@googlemail.com}

Jakub Szefer
School of Engineering & Applied Science, Yale University, United States
{jakub.szefer@yale.edu}

Ali Sunyaev
Information Systems and Systems Engineering, Research Center for IS Design (ITeG),
University of Kassel, Germany, {sunyaev@uni-kassel.de}

ABSTRACT

In an information systems context, information privacy communication will only work if information systems meet the information needs of their users. Since the needs are neither static nor uniform, a promising approach avoiding inadequacies of ignoring differences in users' information needs and more practical than dedicated attention to each individual user is to target information privacy communication to user archetypes. To identify such archetypes, we conduct a survey eliciting users' information needs and apply hierarchical clustering to derive a hierarchical model of user archetypes with respect to their information privacy information needs. We identify a total of 13 archetypes on two hierarchy levels. In contrast to extant research on information privacy user archetypes focusing on information privacy attitudes, the identified information privacy user archetypes are based on information system characteristics desired by users as elicited through our survey. Thus, they yield clear input for enhancing information system design with respect to information privacy. Our research highlights differences and similarities between archetypes and enriches it with an interpretatively derived characterization of the different archetypes. The resulting archetype hierarchy serves as foundation for future research aiming to improve communication of information privacy practices.

Keywords: information privacy, user archetypes, information privacy communication, information privacy information needs, information privacy segregation, information privacy partitioning, information privacy segmentation, hierarchical clustering, privacy enhancing technologies

INTRODUCTION

A fundamental challenge for effective information system design with respect to information privacy communication is to provide users with the right information on the information privacy practices of the information system. If users are not provided with the information they find important with respect to information privacy, they will have no basis to determine whether their information privacy preferences are addressed by the information system and will not perceive the information system to be aligned with their information privacy preferences. In essence, effective communication of information privacy practices is a prerequisite for users to accept an information system as meeting their information privacy needs. Miss-alignment of information contained in information privacy communications with regard to user needs can adversely impact information system adoption.

Effective communication of information privacy practices is challenging due to a lack of a clear conceptualization of information privacy (Solove 2002) and the fluctuations of users' information privacy preferences (Acquisti et al. 2015). Differences in information privacy attitudes between users and variations of user preferences over time and in different contexts may require that users are provided with different information about information privacy practices so they can make decisions whether the information system meets their needs. Moreover, differences in users' conceptualizations of information privacy also induce differences in users' information privacy information preferences.

One potential solution is dedicated communication of information privacy practices to each individual user in a custom-made manner. This is unrealistic as information privacy communications would have to be specifically made for each user, accounting for each users' preferences; such detailed information about each users' desires is likely not available. A promising approach avoiding limitations of one-size-fits-all information privacy communication to all users and also more practical than custom-made communication of information privacy practices to each individual user, is to target communica-

tion of information privacy practices to different user archetypes. This requires, however, a partitioning of the user base into different archetypes and tailoring the communication for each archetype. This work tackles the problem of how to partition the user base into viable archetypes upon which targeted communication of information privacy practices to different users can be made. Actual development of the targeted communication is an orthogonal research problem that we plan to address in separate work.

Prominent extant information privacy user archetypes are given by Westin's partitioning of users into: Fundamentalists, Pragmatists, and Unconcerned (Kumaraguru and Cranor 2005). The three archetypes are, however, only of limited value regarding communication of information privacy practices because they were derived based on surveys on users' information privacy attitudes and not on what different users desire to be contained in information privacy communications. In addition, Westin's partitioning remains quite general so that it is difficult to map the archetypes to information needs. In this research, we identify new, different user archetypes with respect to their information privacy information needs. The objective of this work is to answer the research question: What are the user archetypes with respect to information needs about information privacy practices of information systems?

This work contributes to the scientific knowledge base by identifying a hierarchical model of user archetypes with respect to information privacy information needs, by highlighting characteristic information needs of the different archetypes and by interpretatively deriving succinct, intuitive characterizations of the different user archetypes. For practical audiences, this research facilitates a better understanding of differences in users' information privacy information needs so that information privacy communication can be done better in future designs of information systems.

INFORMATION PRIVACY USER ARCHETYPES

Information Privacy

Information privacy is, for now, best conceptualized as a set of related problems with similar

characteristics but with no universal definition (Solove 2002). For the sake of clarity, in this work we build on the idea of vertical information privacy (Krol and Preibusch 2015). We conceptualize information privacy as a communication relationship between a user and an information system (see Figure 1). This relationship is shaped by the information privacy practices (eg, information collection and processing) of the information system and the perception of them by the user. A salient feature of this conceptualization of information privacy is that it accounts for arbitrary information privacy orientations of information system providers (eg, privacy minimizers or differentiators (Greenaway et al. 2015)) and for arbitrary information privacy conceptualizations employed by users (eg, control-based, commodity-based, or some self-contrived conceptualization). Information privacy practices are determined through information system design and management, and constitute a reflection of information system providers' information privacy orientation. Information privacy perceptions are mainly determined by users' information privacy conceptualization, attention to users' information privacy information needs by information system providers, and fit of implemented information privacy practices with users' preferences for information privacy practices. Hence, according to the employed conceptualization of information privacy, effective information system design accounting for information privacy requires that information system providers communicate their information privacy practices and implement information privacy practices that align with users' preferences for information privacy practices. In this work, we focus on the identification of user archetypes with respect to information privacy information needs as foundation for effective information privacy communica-

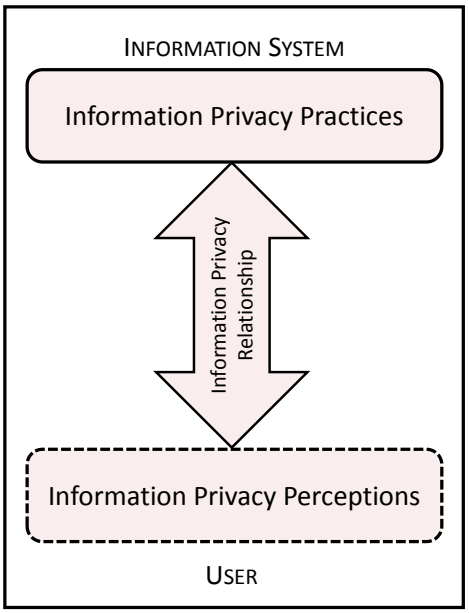

Figure 1. Information privacy as a communication relationship between a user and an information system shaped by users' perceptions of the information systems' information privacy practices.

tions. Users' preferences for information privacy practices are beyond the scope of this work.

Extant Research on Information Privacy User Archetypes

Westin's information privacy partitioning was developed to succinctly convey information privacy attitude survey results and to keep track over changes in information privacy attitudes over time (Kumaraguru and Cranor 2005). Other researchers proposed information privacy user archetypes to investigate the nature of information privacy concerns (Cranor et al. 1999), to map information privacy concerns with internet literacy and social awareness (Dinev and Hart 2006), to interpret information privacy-related online behavior (Adams and Sasse 1999), or to compare stated information privacy preferences to behavioral intentions (Woodruff et al. 2014) or to actual online behavior (Berendt et al. 2005; Spiekermann et al. 2001). These prior attempts partitioning users by information privacy attitudes yield, however, only limited input to understand how to satisfy users' information needs and how users' information needs differ. Hann et al. (2007) took a different approach and partitioned users based on user perceptions of information privacy practices and benefits offered by information systems, which resulted in the archetypes Privacy Guardians, Information Sellers, and Convenience Seekers. In this research, we take a similar approach and partition users based on their information needs with respect to information privacy practices of an information systems. Deriving user archetypes based on information system characteristics desired by users, instead of information privacy attitudes, yields clear implications for enhancing information system design with respect to information privacy because it allows to draw conclusions what information system components related to functionality like management, monitoring, and communication of information privacy practices need to be implemented.

Information Privacy Information Needs

Information needs differ from other types of needs such as the need for food. The latter is a primary human need. An information need can be seen as a secondary need that is an instrument to meet a

primary need (Hjørland 1997). For example, the information needs of users with respect to the information privacy practices of an information system are secondary needs in relation to their primary need for managing their information privacy. Within the scope of this work, we focus on conscious information needs of users with respect to information privacy practices of information systems. We conceptualize information privacy information needs as the wish to be informed whether certain practices perceived as relevant for information privacy are being exercised by an information system or not.

IDENTIFYING ARCHETYPES BY INFORMATION PRIVACY INFORMATION NEEDS

We chose a scenario-based online survey approach to elicit users' information privacy information needs. Information needs were elicited within the context of smartphone applications (apps) because they are targeted to consumers, consumers are used to them, and we conducted the survey with a consumer sample. As we employed a scenario-based approach and did not observe users' information needs in real situations, the survey only elicited information privacy information needs on a general level and results do not reflect situational impacts. To control for situational impacts on users' information privacy information needs, we developed four scenarios with different levels of information sensitivity and perceived privacy. Information sensitivity and perceived privacy were measured with items from Dinev et al. (2013) on 7-point Likert scales. To ensure that survey participants had a similar understanding of the functionality of an app and results were not biased by brand effects, we developed four generic descriptions of four common types of apps (see Table 1).

After a short introduction outlining the study purpose and clarifying the central concepts, the survey elicited prior privacy experiences, information privacy concerns, and behavioral intention to use smartphones with items developed by Xu et al. (2012) on 7-point Likert scales as controls. Then, every survey participant was presented with a randomly selected scenario. For the respective scenario, the survey elicited participants' information privacy information needs with the question: "If you would

Table 1. Employed scenarios with mean (M) and standard deviation (SD) values for information sensitivity and perceived privacy ratings (1=low, 7=high) obtained in the survey.

Scenario	Brief description	Information sensitivity M (SD)	Perceived privacy M (SD)
Calculator	An app offering support to solve simple arithmetic problems.	2.4 (1.8)	5.9 (1.4)
Music streaming	An app to access and stream a large number of music tracks.	4.1 (1.7)	3.9 (1.6)
Navigation	An app to help the user navigate while driving a car.	5.2 (1.8)	3.5 (1.6)
Finance	An app to access a bank account and make financial transactions.	6.1 (1.6)	2.8 (2.0)

use such an app, how important would it be for you to be informed about the following aspects?" The aspects listed below the question were focused on different information privacy practices derived from a literature review and a review of privacy policies conducted in previous research (Dehling et al. 2014; Sunyaev et al. 2015). Information privacy practices were organized by major information privacy concerns, information collection, handling of information, rationale for information privacy practices, and offered privacy controls (Ackerman et al. 1999; Antón et al. 2010). Five information privacy practices focused on sensors used for information collection. Five other information privacy practices focused on type of information collected. Another five information privacy practices focused on handling of information. Seven aspects focused on rationale for information privacy practices. Nine information practices focused on offered privacy controls. Participants gave their answers on a 101-point slider scale (0 = unimportant, 100 = very important). All survey materials are available from the authors upon request. To ensure survey item comprehensibility a pretest was conducted.

The survey was conducted in June and July 2016 in Germany. Participants were recruited over social media channels. 160 participants completed the online questionnaire. 26 participants failed to correctly answer a control question and were excluded. 134 participants (female=73, male=60, unknown=1) remained for data analysis. Participant age ranged from 18-24 to 65-70 years (18-24 (39, 29.1%); 25-29 (51, 38.1%); 30-34 (8, 6%); 35-39 (6, 4.5%); 40-44 (2, 1.5%); 45-49 (5, 3.7%); 50-54 (7, 5.2%); 55-59 (6, 4.5%); 60-64 (6, 4.5%); 65-70 (3, 2.2%)). Most participants had an university degree as highest degree (university degree (79, 59%); students (28, 20.9%); completed vocational train-

ing (14, 10.4%); other (13, 9.7 %)). Two participants did not regularly use smartphone apps.

To identify the user archetypes, we employed an agglomerative hierarchical clustering algorithm (Ward 1963). Participants with the smallest difference in the variance of their responses were iteratively grouped. Afterwards, we inspected the resulting hierarchical order and calculated mean values and standard deviations of participant responses for all resulting clusters. Finally, one researcher interpreted information needs that stood out for identified clusters (eg, high mean responses or small standard deviations), coined a name for the archetype, and developed a brief interpretative description of the archetype. To ensure that archetype names and descriptions are intuitive and fit the data, three other researchers reviewed archetype names and descriptions. Based on their feedback, archetype names and descriptions were iteratively refined and improved until all researchers were satisfied with the result.

USER ARCHETYPES BY INFORMATION PRIVACY INFORMATION NEEDS

The clustering algorithm identified 13 archetypes. Figure 2 presents an overview of the archetypes and their descriptions. Three archetypes form the top level of the hierarchy: Guarded Information Seekers (three subordinate archetypes), Pragmatic Information Seekers (four subordinate archetypes), and Committed Information Seekers (three subordinate archetypes).

Table 2 presents the number of participants by archetype and scenario. 15.7% (21/134) of participants are classified as Guarded Information Seekers, 38.8% (52/134) of participants are classified as Pragmatic Information Seekers, and 45.5% (61/134) of participants are classified as Committed Information Seekers.

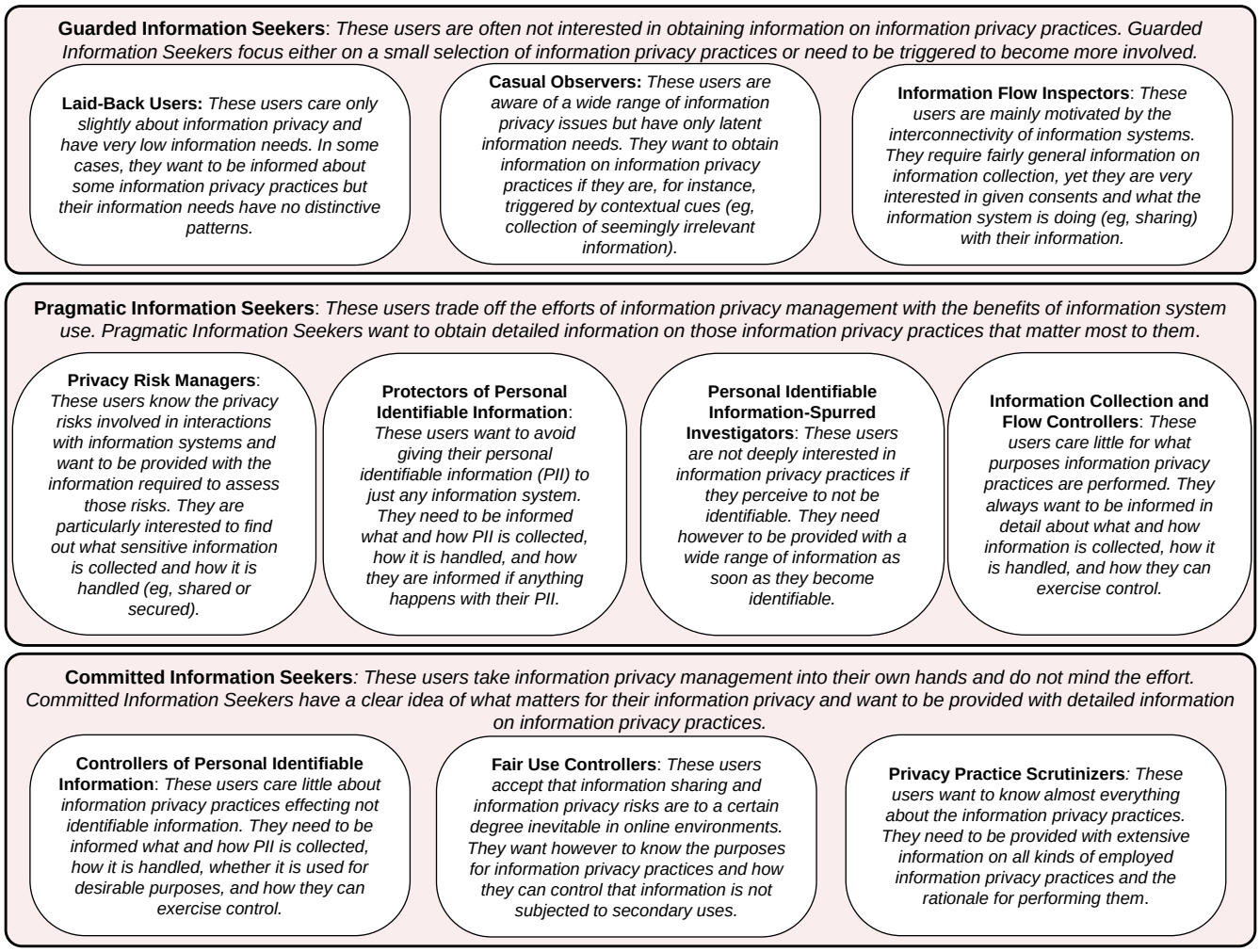

Figure 2. Overview of identified archetypes with names and illustrative descriptions.

Table 3 presents mean values and standard deviations for users' reported information privacy information needs for all archetypes. Characteristic information needs are highlighted. Across all archetypes users are most interested in collection of information about users (M=83.6, SD=23.5), information sharing (M=83.6, SD=26.1), consent management (M=80.5, SD=24.2), information privacy breach notification (M=80.3, SD=24.7), and access to collected information (M=79.3, SD=22.8). Users are least interested in privacy policy change governance (M=58.2, SD=30.4), whether information privacy practices are carried out for technical purposes (M=56.0, SD=31.04) or for social welfare (M=51.5, SD=32.5), and in data formats used for information collection (M=49.9, SD=32.5).

Which scenario was presented has no meaningful or significant impact on archetypes (Spearman

Table 2. Number of study participants by archetype and scenario n (%).

Guarded Information Seekers	Pragmatic Information Seekers	Committed Information Seekers

$\rho = 0.101$, $p = 0.245$, scenarios ranked by information sensitivity and archetypes ranked by mean information needs). Age (two-sided Fisher's Exact test $p = 0.139$), gender (two-sided Fisher's Exact test $p = 0.742$), and level of education (Spearman $\rho = -0.141$, $p = 0.106$) also have no meaningful and no significant impact on archetypes. Behavioral intention to use smartphones (Spearman $\rho = -0.251$, $p = 0.003$) and reported frequency of smartphone use (Spearman $\rho = -0.233$, $p = 0.007$) have a weak negative correlation with mean information needs of archetypes. Prior privacy experience (Spearman $\rho = 0.267$, $p = 0.002$) and information privacy concerns (Spearman $\rho = 0.314$, $p < 0.001$) have a weak positive correlation with mean information needs of archetypes.

	Laid-Back Users	Casual Observers	Information Flow Inspectors	Privacy Risk Managers	Protectors of Personal Identifiable Information	Personal Identifiable Information-Spurred Investigators	Information Collection and Flow Controllers	Controllers of Personal Identifiable Information	Fair Use Controllers	Privacy Practice Scrutinizers	Total
Calculator	3 (75.0)	4 (40.0)	2 (28.6)	2 (20.0)	2 (13.3)	7 (31.8)	1 (20.0)	3 (16.7)	3 (16.7)	4 (16.0)	31 (23.1)
Music Streaming	0 (0.0)	3 (30.0)	3 (42.9)	1 (10.0)	1 (6.7)	5 (22.7)	3 (60.0)	6 (33.3)	3 (16.7)	10 (40.0)	35 (26.1)
Navigation	1 (25.0)	2 (20.0)	0 (0.0)	5 (50.0)	6 (40.0)	7 (31.8)	1 (20.0)	3 (16.7)	7 (38.9)	5 (20.0)	37 (27.6)
Finance	0 (0.0)	1 (10.0)	2 (28.6)	2 (20.0)	6 (40.0)	3 (13.6)	0 (0.0)	6 (33.3)	5 (27.8)	6 (24.0)	31 (23.1)
Total	4 (3.0)	10 (7.5)	7 (5.2)	10 (7.5)	15 (11.2)	22 (16.4)	5 (3.7)	18 (13.4)	18 (13.4)	25 (18.7)	134 (100.0)
	21 (15.7)			52 (38.8)				61 (45.5)			

DISCUSSION

The main finding of our research is that users' information privacy information needs differ widely between users. Some users have fairly low information needs and show only latent interests in

Table 3. Reported information privacy information needs by archetype mean (M) and standard deviation (SD) values. Information needs interpreted as characteristic for an archetype are in bold font.

	Guarded Information Seekers			**Pragmatic Information Seekers**				**Committed Information Seekers**		
	Laid-Back Users	**Casual Observers**	**Information flow inspectors**	**Privacy risk managers**	**Protectors of personal identifiable information**	**Personal identifiable information-spurred investigators**	**Information collection and flow controllers**	**Controllers of personal identifiable information**	**Fair use controllers**	**Privacy practice scrutinizers**
Handling of information	4.5 (4.6)	54.7 (21.1)	**79.7 (26.4)**	65.4 (28.7)	85.4 (19.4)	59.5 (27.2)	**98.2 (3.6)**	**92.2 (7.6)**	**87.0 (15.8)**	**94.5 (9.8)**
> Information retention	2.5 (4.3)	**30.2 (11.3)**	48.0 (30.2)	41.2 (33.5)	72.4 (20.8)	42.9 (25.9)	**94.0 (12.0)**	73.0 (26.0)	58.7 (33.7)	**92.2 (10.6)**
> Information security	2.5 (4.3)	**43.4 (15.8)**	67.3 (18.4)	**83.5 (10.0)**	73.9 (19.4)	57.4 (26.3)	**96.6 (6.8)**	**90.0 (10.0)**	73.9 (27.7)	**94.0 (10.8)**
> Information sharing	1.3 (2.2)	**45.5 (15.1)**	**90.1 (11.2)**	**82.5 (14.7)**	**93.2 (9.4)**	**75.0 (27.6)**	**100 (0.0)**	90.2 (22.8)	**92.4 (8.0)**	**98.3 (4.3)**
> Information storage	1.3 (2.2)	34.5 (21.4)	**70.4 (24.0)**	47.1 (24.3)	61.6 (26.8)	56.0 (32.3)	**96.6 (6.8)**	65.3 (29.1)	76.6 (20.1)	**94.8 (7.1)**
Information collection sensors	2.5 (4.3)	**31.5 (9.3)**	71.6 (17.9)	18.2 (17.7)	81.9 (18.0)	59.1 (18.1)	**90.2 (8.3)**	**86.8 (13.4)**	69.1 (21.9)	**94.3 (9.2)**
> Environment sensors	1.3 (2.2)	**35.5 (9.6)**	49.1 (34.0)	24.3 (23.8)	74.1 (21.8)	61.5 (19.6)	**98.8 (1.6)**	83.9 (17.5)	74.3 (21.1)	**94.2 (7.7)**
> Location sensors	26.0 (42.8)	**39.6 (14.8)**	63.1 (31.5)	44.1 (33.7)	70.4 (22.5)	68.5 (18.7)	**82.6 (18.4)**	82.3 (19.7)	77.2 (19.7)	**97.0 (5.6)**
> User sensors	38.0 (40.4)	**39.8 (14.2)**	61.9 (31.7)	50.0 (28.2)	**86.5 (13.0)**	**72.5 (19.4)**	**97.0 (6.0)**	**94.2 (10.6)**	78.1 (24.9)	**98.7 (2.6)**
> Software use sensors	1.0 (1.7)	**33.0 (7.2)**	40.1 (27.7)	22.8 (25.1)	64.1 (22.1)	50.7 (20.9)	**93.2 (8.4)**	79.3 (15.7)	74.5 (19.7)	92.7 (13.2)
Type of collected information	10.0 (13.1)	39.9 (16.7)	69.6 (28.3)	67.1 (22.0)	76.4 (26.8)	**78.0 (14.2)**	**99.8 (0.4)**	**91.5 (12.9)**	**87.3 (12.6)**	93.2 (19.6)
> Different formats of data collected	1.5 (2.6)	**21.2 (12.9)**	19.1 (23.8)	17.0 (20.5)	35.1 (25.9)	45.3 (21.2)	70.6 (25.1)	64.1 (29.7)	68.9 (19.8)	75.7 (25.0)
> Collection of user identifiers	4.0 (4.2)	**41.0 (13.5)**	37.6 (36.1)	57.6 (28.8)	**91.7 (9.4)**	**76.5 (17.0)**	74.6 (38.7)	**97.0 (6.8)**	79.6 (24.4)	92.9 (20.6)
> Information collected for information system operation	11.5 (16.6)	32.5 (18.7)	41.6 (24.7)	51.2 (24.6)	56.5 (34.5)	67.0 (16.6)	78.2 (20.0)	84.8 (17.8)	73.4 (21.4)	88.9 (21.2)
> Information on the user	35.0 (39.4)	**44.5 (14.1)**	60.4 (33.2)	**88.4 (8.0)**	**92.5 (8.9)**	**78.5 (13.6)**	**100 (0.0)**	**97.8 (4.2)**	82.2 (23.4)	**98.2 (4.5)**
Offered privacy controls	13.8 (21.0)	**49.0 (15.4)**	41.9 (32.7)	63.5 (26.2)	**77.1 (25.2)**	**70.1 (17.0)**	80.0 (40.0)	74.2 (21.1)	80.4 (16.7)	**96.8 (6.6)**
> Breach notification	13.3 (21.3)	**46.2 (12.1)**	59.1 (20.2)	59.4 (24.1)	**90.4 (13.5)**	**75.4 (17.3)**	**97.0 (3.8)**	**90.6 (13.4)**	**91.0 (9.4)**	**98.8 (2.9)**
> Privacy policy change governance	0.8 (1.3)	**24.4 (6.8)**	13.0 (16.8)	51.3 (25.4)	46.3 (19.4)	54.0 (17.0)	**91.0 (11.1)**	54.4 (27.0)	77.9 (16.6)	89.4 (11.9)
> Privacy policy change notification	1.0 (1.7)	41.5 (17.6)	36.3 (30.8)	67.9 (19.6)	54.0 (23.6)	63.7 (12.5)	**99.0 (2.0)**	69.6 (25.0)	79.8 (18.7)	**94.1 (9.5)**
> Consent management	13.5 (21.1)	**49.4 (10.1)**	**83.7 (15.8)**	65.4 (26.1)	**79.9 (15.3)**	**79.4 (15.6)**	**93.8 (12.4)**	84.6 (23.8)	**88.6 (9.3)**	**98.6 (4.1)**
> Downstream propagation	1.3 (1.6)	**32.5 (13.0)**	66.3 (29.7)	61.6 (25.4)	64.5 (26.7)	**74.1 (16.3)**	**99.6 (0.5)**	80.2 (16.6)	**88.2 (11.4)**	**95.7 (7.8)**
> Privacy practice monitoring	1.0 (1.7)	45.3 (17.2)	52.3 (33.4)	67.2 (26.6)	49.1 (20.0)	68.6 (21.8)	**92.4 (15.2)**	**86.9 (12.9)**	83.8 (14.9)	**94.6 (9.2)**
> Secondary use consent	5.0 (8.7)	42.1 (21.4)	**78.9 (17.9)**	67.5 (28.4)	63.6 (21.4)	68.1 (14.0)	**100 (0.0)**	**87.1 (13.0)**	**88.8 (8.9)**	**95.8 (7.9)**
> User access	31.3 (32.5)	41.5 (20.2)	61.9 (26.7)	**85.4 (7.4)**	**78.5 (16.6)**	69.8 (17.4)	**93.2 (8.4)**	**88.4 (12.8)**	**90.1 (8.3)**	**96.3 (7.1)**
Practice rationale	1.5 (2.6)	29.2 (18.1)	32.4 (31.5)	54.0 (28.4)	48.1 (26.0)	54.9 (20.6)	35.2 (40.6)	63.4 (20.1)	83.5 (15.9)	88.3 (14.2)
> Communication	43.8 (44.6)	**38.6 (9.3)**	22.3 (26.3)	41.5 (26.5)	40.3 (23.5)	61.4 (19.2)	32.8 (29.1)	55.4 (28.5)	**85.3 (12.1)**	**90.7 (11.3)**
> Offered service	28.3 (28.0)	**47.7 (9.5)**	10.4 (14.2)	71.2 (25.6)	46.6 (24.5)	66.3 (21.0)	37.6 (38.8)	81.3 (18.5)	**87.2 (13.1)**	**92.2 (9.5)**
> Personalization	30.0 (32.1)	**49.3 (15.0)**	24.1 (27.1)	69.4 (16.9)	48.7 (27.5)	61.8 (22.0)	8.6 (11.8)	73.7 (31.4)	78.7 (14.2)	**93.1 (9.2)**
> Public welfare	19.0 (32.9)	**31.1 (13.2)**	16.3 (23.7)	66.7 (18.8)	26.3 (21.2)	53.4 (22.4)	3.8 (7.6)	43.2 (26.4)	73.5 (25.1)	81.6 (22.2)
> Service operation	22.3 (31.0)	**45.0 (5.3)**	26.4 (25.9)	70.4 (20.0)	51.5 (22.3)	52.8 (19.8)	24.0 (38.8)	71.7 (26.3)	**82.8 (13.4)**	87.8 (16.8)
> Technical details	30.5 (32.3)	**45.4 (11.8)**	27.3 (23.6)	55.8 (32.2)	44.3 (29.6)	54.6 (19.5)	4.4 (8.8)	44.1 (29.6)	80.9 (15.6)	81.7 (18.6)

certain information privacy practices, others have very strong interests for a small selection of information privacy practices, and some users need to be informed about a wide range of information privacy practices. We identified a total of 13 archetypes split over two hierarchy levels. Through iterative development of archetype names and succinct descriptions in a final interpretative step, this research also demonstrates that information privacy information needs serve as useful foundation to develop a better understanding of the user base. The study highlights differences and similarities between archetypes and enriches it with an interpretatively derived characterization of the different archetypes.

Furthermore, this research demonstrates the utility of hierarchical clustering to identify information privacy user archetypes. While main information needs between the top level archetypes mostly differ only in intensity but not in type of information need, the second level archetypes paint a more refined picture and allow for clearer distinctions between archetypes. Some information privacy practices seem to be of interest to the majority of users (eg, information sharing, collection of user information) and others seem to be of only limited interest to the majority of users (eg, data formats used for information collection, carrying out information privacy practices for social welfare). The hierarchical archetypes do not only reflect these common information needs but tease out more hidden characteristics of user groups focusing on combinations of information needs.

Implications for Theory

This research contributes mainly to extant research on information privacy user archetypes. We introduce information privacy information needs as foundation to identify information privacy user archetypes that yield insights for how to improve information system design with respect to communication of information privacy practices. The identified information privacy user archetypes demonstrate that the user base consists of very different users with respect to information privacy information needs. The conducted research serves as foundation for future research aiming to improve communication of information privacy practices by giving an overview of differences in information privacy information

needs that purposeful privacy enhancing technologies need to cater to. Furthermore, this research demonstrates the utility of the concept of vertical information privacy for information systems research.

From an information systems perspective, information privacy is in essence a relationship between a user and an information system. In the end, it will not matter whether users have the 'right' conceptualization of information privacy or not. Information systems depend on users and thus, from an information privacy perspective, they have to be designed in such a way that they are compatible with the information privacy conceptualizations of users. The information privacy user archetypes identified based on users' information needs can be used as a first step to accomplish this.

Implications for Practice

This research supports practical audiences and policy makers to better understand the user base their information systems are catering too. Users have very different information needs when it comes to information privacy. This should also be reflected in information system design. Information system providers must not only craft information privacy practices that align with users' information privacy preferences, but they also need to focus on effective and efficient ways to communicate their information privacy practices. This is not the posting of long and confusing privacy notices but rather dedicated tools that fit the specific needs of relevant user groups. Better communication practices for information sharing, consent management, and breach notification, especially, if personal identifiable information is involved, seem like a promising first step as these were of interest to users across the board.

Limitations

We cannot assess whether more meaningful archetypes exist on the current or deeper levels of the archetype hierarchy due to the sample size. However, since we already found 13 archetypes with a sample size similar to those used for extant research on information privacy user archetypes, we expect that the used approach would yield even better results with a larger sample size. The analyses with re-

spect to socio-demographic factors should be treated with care as we focused on identification of different user archetypes and not on the identification of user archetypes present in a sample that is representative for a certain population. Furthermore, we did not assess why users have certain information needs due to the research focus on deriving archetypes based on similarities in information needs. Finally, this study only assesses information privacy information needs on a general level and not in the context of real situations. As indicated by the absence of a meaningful correlation between scenarios and participant archetypes, presented scenarios had no significant impact on users' information needs. We expect that users will change between archetypes depending on situational cues if real situations with real information privacy implications are observed. The objective of this study was however to identify different archetypes and not to assess what archetypes exist in different contexts.

Future Research

Among the most promising opportunities for future research are quantitative studies with larger sample sizes to test whether more archetypes can be identified, qualitative studies to characterize the different archetypes in depth, design science research to develop privacy enhancing tools for communication of information privacy practices tailored to different archetypes, and research on how information privacy user archetypes differ across situational and individual influences. It will also be interesting to investigate how users' information privacy information needs are formed. All control items tested in this study had at most weak correlations with users' information needs. This indicates that information privacy information needs are either formed by complex processes or depend mainly on influences this study did not control for.

Conclusion

Implementing effective information privacy communication is a challenging, yet achievable, task. Information processing and information system design is not dictated by nature but chosen by information system designers (Cohen 2000; Dehling et al. 2015). A better understanding of users' infor-

mation privacy information needs, as offered by the identified information privacy user archetypes, will be helpful to build information systems that account for information privacy and are in the end more beneficial for all involved through effective information privacy communication.

ACKNOWLEDGEMENTS

This project was supported by the Kompetenzzentrum Verbraucherforschung NRW research grant 324-8.03.02.02.03-125085 from Ministry for Climate Protection, Environment, Agriculture, Conservation and Consumer Protection of the State of North Rhine-Westphalia, Verbraucherzentrale Nordrhein-Westfalen, and Ministry for Innovation, Science and Research of the State of North Rhine-Westphalia.

REFERENCES

Ackerman, M. S., Cranor, L. F., and Reagle, J. 1999. "Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences," in *1st ACM Conference on Electronic Commerce*, Denver, CO, USA: ACM, November 3, pp. 1–8 (doi: 10.1145/336992.336995).

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information," *Science* (347:6221), pp. 509–514 (doi: 10.1126/science.aaa1465).

Adams, A., and Sasse, M. A. 1999. "Privacy Issues in Ubiquitous Multimedia Environments: Wake Sleeping Dogs or Let Them Lie," in *Proceedings of Interact '99*, Edinburgh, Scotland: IOS Press, September 30, pp. 214–221.

Antón, A. I., Earp, J. B., and Young, J. D. 2010. "How Internet Users' Privacy Concerns Have Evolved Since 2002," *IEEE Security & Privacy* (8:1), pp. 21–27 (doi: 10.1109/MSP.2010.38).

Berendt, B., Günther, O., and Spiekermann, S. 2005. "Privacy in e-Commerce: Stated Preferences vs. Actual Behavior," *Communications of the ACM* (48:4), pp. 101–106 (doi: 10.1145/1053291.1053295).

Cohen, J. E. 2000. "Examined Lives: Informational Privacy and the Subject as Object," *Stanford Law Review* (52:5), pp. 1373–1438 (doi: 10.2307/1229517).

Cranor, L. F., Reagle, J., and Ackerman, M. S. 1999. "Beyond Concern: Understanding Net Users' Attitudes about Online Privacy," No. TR 99.4.3, AT&T Labs-Research Technical Report, Cambridge, MA, USA: MIT Press (available at http://arxiv.org/html/cs/9904010/report.htm).

Dehling, T., Gao, F., Schneider, S., and Sunyaev, A. 2015. "Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Applications on iOS and Android," *JMIR mHealth uHealth* (3:1), p. e8 (doi: 10.2196/mhealth.3672).

Dehling, T., Gao, F., and Sunyaev, A. 2014. "Assessment Instrument for Privacy Policy Content: Design and Evaluation of PPC," in *Proceedings of the Pre-ICIS Workshop on Information Security and*

Privacy, Auckland, New Zealand: AIS, December 13.

Dinev, T., and Hart, P. 2006. "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact," *International Journal of Electronic Commerce* (10:2), pp. 7–29 (doi: 10.2753/JEC1086-4415100201).

Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2013. "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts," *European Journal of Information Systems* (22:3), pp. 295–316 (doi: 10.1057/ejis.2012.23).

Greenaway, K. E., Chan, Y. E., and Crossler, R. E. 2015. "Company Information Privacy Orientation: A Conceptual Framework," *Information Systems Journal* (25:6), pp. 579–606 (doi: 10.1111/isj.12080).

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., and Png, I. P. L. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach.," *Journal of Management Information Systems* (24:2), pp. 13–42 (doi: 10.2753/MIS0742-1222240202).

Hjørland, B. 1997. *Information Seeking and Subject Representation*, Westport, CT, USA: Greenwood Press.

Krol, K., and Preibusch, S. 2015. "Effortless Privacy Negotiations," *IEEE Security & Privacy* (13:3), pp. 88–91 (doi: 10.1109/MSP.2015.51).

Kumaraguru, P., and Cranor, L. F. 2005. "Privacy Indexes: A Survey of Westin's Studies," *ISRI Technical Report* (available at http://www.casos.cs.cmu.edu/publications/papers/CMU-ISRI-05-138.pdf).

Solove, D. J. 2002. "Conceptualizing Privacy," *California Law Review* (90:4), pp. 1087–1155 (doi: 10.15779/Z382H8Q).

Spiekermann, S., Grossklags, J., and Berendt, B. 2001. "E-privacy in 2nd Generation E-commerce: Privacy Preferences Versus Actual Behavior," in *Proceedings of the 3rd ACM Conference on Electronic Commerce*, New York, NY, USA: ACM, pp. 38–47 (doi: 10.1145/501158.501163).

Sunyaev, A., Dehling, T., Taylor, P. L., and Mandl, K. D. 2015. "Availability and Quality of Mobile Health App Privacy Policies," *Journal of the American Medical Informatics Association* (22:e1), pp. e28–e33 (doi: 10.1136/amiajnl-2013-002605).

Ward, J. H. 1963. "Hierarchical Grouping to Optimize an Objective Function," *Journal of the American Statistical Association* (58:301), pp. 236–244 (doi: 10.1080/01621459.1963.10500845).

Woodruff, A., Pihur, V., Consolvo, S., Schmidt, L., Brandimarte, L., and Acquisti, A. 2014. "Would a Privacy Fundamentalist Sell Their DNA for $1000...If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences," in *Symposium on Usable Privacy and Security*, Menlo Park, CA, USA: USENIX Association, July 9.

Xu, H., Gupta, S., Rosson, M. B., and Carroll, J. M. 2012. "Measuring Mobile Users' Concerns for Information Privacy," in *Proceedings of the Thirty Third International Conference on Information Systems (ICIS 2012)*, Orlando, FL, U.S., December 16.